View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

ELSEVIER
Theoretical Computer Science 183 (1997) 83–92
Theoretical Computer Science

# A note on decidability questions on presentations of word semigroups

C. Choffrut[a], T. Harju[b], J. Karhumäki[b,*,1]

[a] *Université Paris VII, LITP, 2, place Jussieu, 75251 Paris Cedex 05, France*
[b] *Department of Mathematics, University of Turku, Yliopistonmaki FIN-20014 Turku, Finland*

**Abstract**

We apply automata-theoretic tools and some recently established compactness properties in the study of F-semigroups, that is, subsemigroups of free semigroups. With each F-semigroup we associate an F-presentation, which turns out to be finite for all finitely generated F-semigroups. Connections between F-presentations and ordinary presentations of semigroups are pointed out. It is also shown that it is undecidable whether two finitely generated F-semigroups satisfy a common relation in their F-presentations.

## 1. Introduction

Our goal here is to consider certain properties of subsemigroups of free semigroups, that is, of *F-semigroups*. These properties are established using automata-theoretic tools and these have become natural after the proof of the compacteness result of free semigroups by Albert and Lawrence [1] and by Guba [7].

Most of the results of this paper are simple, after our approach is taken, and most of them are known in the literature, see e.g. [8, 9, 15]. We shall give here a short unified presentation of the topic which also reveals some interesting open problems. Also, we prove a new undecidability result for F-semigroups that states that there is no algorithm to determine whether two finitely generated F-semigroups share a relation in their F-presentations.

Let $A \subseteq \Sigma^+$ be a set of words, and $X$ a set of letters. Consider a pair $(u, v) \in X^+ \times X^+$ as an equation $u = v$ in the variables $x \in X$ that take their values from $\Sigma^+$, so that a morphism $\alpha : X^+ \to \Sigma^+$ is a solution of $u = v$ if and only if $\alpha(u) = \alpha(v)$. We can then define the *equivalence* of two relations $R_1, R_2 \subseteq X^+ \times X^+$ simply by requiring that they have the same solutions as systems of equations. This yields, due to the mentioned

* Corresponding author.
[1] Partially done when this author visited at the Universitè Paris VII and supported by Academy of Finland, grant 14047.

0304-3975/97/$17.00 © 1997 — Elsevier Science B.V. All rights reserved
*PII* S0304-3975(96)00311-8

compactness result, a finite F-presentation $[X,R]$ to each finitely generated F-semigroup. Moreover, simple automata-theoretic observations show that such a finite F-presentation can always be found effectively, which, in turn, implies that the isomorphism problem is decidable for finitely generated F-semigroups.

The approach taken above does not seem to generalize to rationally generated F-semigroups. Indeed, it seems to be an open problem whether two F-semigroups generated by rational sets are isomorphic, although the restricted problem of determining whether a rationally generated F-semigroup is free is a well known decidable problem.

Contrary to the isomorphism problem of finitely generated F-semigroups the problem whether two such F-semigroups satisfy a common relation (in their F-presentations) turns out to be undecidable. In order to prove this we need the undecidability of the Post Correspondence Problem for injective morphisms; see [13]. It is interesting to note that here we need the PCP for injective morphisms, but the problem itself is not just an injective variant of a more general problem.

## 2. F-presentations

We begin with some general notions of semigroup presentations, see e.g. [12] for a more comprehensive study of these.

Let $S$ be a semigroup generated by a set $U$, and let $\varphi : X \to U$ be a bijection from an alphabet $X$ onto $U$. Since $X$ generates a free semigroup $X^+$ the map $\varphi$ extends uniquely to a morphism $\varphi : X^+ \to S$ onto $S$ such that $S$ is isomorphic to the quotient $X^+/\ker(\varphi)$, where $\ker(\varphi) = \{(u,v) \mid \varphi(u) = \varphi(v)\}$ is the kernel of the morphism $\varphi$. If $R \subseteq X^+ \times X^+$ is a relation such that $\ker(\varphi)$ is the congruence of $X^+$ generated by $R$, then the pair $\langle X;R\rangle$ is a *presentation of $S$ in generators $X$ and defining relations $R$*. We denote this by writing $S = \langle X;R\rangle^{\varphi}$. In particular, $\langle X;\ker(\varphi)\rangle$ is a presentation of $S$. It is well known, and easy to see, that two semigroups have a common presentation if and only if they are isomorphic. A presentation $\langle X;R\rangle$ is *finite*, if both the generator set $X$ and the set $R$ of defining relations are finite.

We mention at this point the general algebraic fact that two relations $R_1, R_2 \subseteq X^+ \times X^+$ generate the same congruence if and only if for all morphisms $\beta : X^+ \to S$ into an arbitrary semigroup, one has

$$R_1 \subseteq \ker(\beta) \;\Leftrightarrow\; R_2 \subseteq \ker(\beta). \tag{1}$$

A subset $A \subseteq \Sigma^+$ generates a subsemigroup $A^+$ of $\Sigma^+$, and conversely, each subsemigroup of $\Sigma^+$ is of this form. We say that a semigroup $S$ is an *F-semigroup*, if it is a subsemigroup of a free semigroup $\Sigma^+$. It is well know that for all F-semigroups $A^+$ the set $\mathscr{B}(A) = A^+ \setminus (A^+)^2$ is the unique minimal generating set for $A^+$, that is, $\mathscr{B}(A)^+ = A^+$ and

$$\forall C : \; C \subset \mathscr{B}(A) \;\Rightarrow\; C^+ \subset A^+,$$

where $\subset$ denotes the proper inclusion.

Let $\varphi : X \to A$ be a bijection. Again, it can be extended to a morphism $\varphi : X^+ \to A^+$ so that the pair $\langle X; \ker(\varphi)\rangle$ is a presentation of $A^+$, that is, $A^+ = \langle X; \ker(\varphi)\rangle^\varphi$.

In the following we assume that $\Sigma$ *is an alphabet with at least two letters.* This is no restriction for us, since clearly for all sets of words $A$, $A \subseteq \Sigma^+$ for some such alphabet $\Sigma$. The assumption that $\Sigma$ has at least two letters is used later to ensure that each finitely generated word semigroup $X^+$ can be embedded into $\Sigma^+$.

We say that two relations $R_1, R_2 \subseteq X^+ \times X^+$ are *equivalent in* $\Sigma^+$, if for any morphism $\alpha : X^+ \to \Sigma^+$,

$$R_1 \subseteq \ker(\alpha) \quad \Leftrightarrow \quad R_2 \subseteq \ker(\alpha). \tag{2}$$

Each pair $(u, v) \in X^+ \times X^+$ can be thought of as an *equation* $u = v$ over the variables in $X$, and a relation $R \subseteq X^+ \times X^+$ becomes then a system of equations over $X$. A solution of an equation $u = v$ is a morphism $\alpha : X^+ \to \Sigma^+$ such that $\alpha(u) = \alpha(v)$. In this way two relations $R_1$ and $R_2$ are equivalent if and only if they have exactly the same solutions as systems of equations.

The following lemma shows that each finitely generated F-semigroup has a rational presentation, that is, a presentation $\langle X; R\rangle$, where $R$ is a rational relation; cf. [2].

**Lemma 2.1.** *Let $A^+$ be an F-semigroup for a finite $A \subseteq \Sigma^+$, and let $\varphi : X \to A$ be a bijection. Then* $\ker(\varphi)$ *is a rational subset of $X^+ \times X^+$. Moreover, one can effectively find a finite equivalent subrelation of* $\ker(\varphi)$.

**Proof.** Now, $\ker(\varphi) = \varphi^{-1}\varphi$, and hence $\ker(\varphi)$ is a rational relation. Indeed, the finite transducer $T$ for $\ker(\varphi)$ accepts all double factorizations of a word $w \in X^+$, that is, $T$ accepts $(u, v)$ if and only if $\varphi(u) = \varphi(v)$. Assume that $T$ has $q$ states. Let $K_0(A) \subseteq \ker(\varphi)$ be obtained from the computations of $T$ of length at most $2q$. It can be now shown using a combinatorial lemma on words that $K_0(A)$ is a required finite equivalent subrelation. For more details of this, see e.g. [4]. □

The second claim of Lemma 2.1 is an effective special case of the Ehrenfeucht's Compactness Property, for the proof of which we refer to [1] or [7]. This result states that for each $R \subseteq X^+ \times X^+$ there exists a finite subrelation $R_0 \subseteq R$ which is equivalent to $R$. Note, however, that the proof of Lemma 2.1 is self-contained, that is, the general compactness property is not needed in its proof.

Note that Lemma 2.1 does not imply that $\langle X; K_0(A)\rangle$ is a presentation of $A^+$. Indeed, the smallest congruence of $X^+$ containing $K_0(A)$ may be properly contained in $\ker(\varphi)$, since by (2), Lemma 2.1 takes care only of those congruences that are generated by the morphisms $\alpha : X^+ \to S$ into the free semigroups $S = \Sigma^+$ instead of all semigroups as required in (1).

We say that $[X; R]$ is an *F-presentation* of $A^+ \subseteq \Sigma^+$, if

(i) there is a bijection $\varphi : X \to A$ such that $R \subseteq \ker(\varphi)$, and

(ii) $R$ is equivalent to $\ker(\varphi)$.

A pair $(u, v) \in \ker(\varphi)$ is called a *relation in the F-presentation* $[X; R]$ of $A^+$.

Actually, in view of (2), an F-presentation $[X;R]$ of $A^+$ uniquely determines $A^+$ up to isomorphism, that is, modulo the presenting bijection $\varphi: X \to A$. Thus, we can write

$$A^+ = [X;R]^\varphi.$$

The following result is now obvious.

**Lemma 2.2.** *Two F-semigroups have a common F-presentation $[X;R]$ if and only if they are isomorphic.*

## 3. Comparison of F-presentations and ordinary presentations

We shall give now a congruence characterization of F-presentations. It is a general algebraic property that congruences $\rho$ of a semigroup $S$ are exactly the kernels of the morphisms $\alpha: S \to P$ for semigroups $P$. We follow Dubreil [6] and say that a congruence $\rho \subseteq S \times S$ is a *nuclear congruence*, if it is the kernel of an endomorphism $\alpha: S \to S$.

**Theorem 3.1.** *Let $A^+ = [X;R]^\varphi$. Then $\ker(\varphi)$ is the smallest nuclear congruence of $X^+$ that contains $R$.*

**Proof.** Let $A \subseteq \Sigma^+$. Now, if $X$ has at least two elements, then there exists an embedding $\iota: \Sigma^+ \to X^+$. In this case, $\iota\varphi: X^+ \to X^+$ is an endomorphism such that $\ker(\varphi) = \ker(\iota\varphi)$, and, consequently, $\ker(\varphi)$ is a nuclear congruence of $X^+$. On the other hand, if $X = \{x\}$ contains only one element, then $A^+$ is a free semigroup (generated by $\varphi(x)$), and $\ker(\varphi)$ is the identity mapping, and thus a kernel of the identity endomorphism of $X^+$. Therefore, $\ker(\varphi)$ is a nuclear congruence of $X^+$.

By the definition of an F-presentation, $R \subseteq \ker(\varphi)$. Further, if $\beta: X^+ \to X^+$ is an endomorphism with $R \subseteq \ker(\beta)$, then, since $\ker(\varphi)$ is equivalent to $R$, $\ker(\varphi) \subseteq \ker(\beta)$ by (2). This proves the claim. □

Our next result states that we can always move from a presentation of an F-semigroup $A^+$ to an F-presentation of $A^+$.

**Lemma 3.2.** *Let $S$ be a semigroup presented by $\langle X;R\rangle$.*

(1) *If $[X;R]$ is an F-presentation of the F-semigroup $A^+$, then $A^+$ is a morphic image of $S$.*

(2) *If $S$ is an F-semigroup, then $S$ is isomorphic to $A^+$.*

**Proof.** Let $S = \langle X;R\rangle^\psi$, where $\psi: X^+ \to S$, and let $A^+ = [X;R]^\varphi$, where $\varphi: X^+ \to A^+$. Since $R \subseteq \ker(\varphi)$, and $\ker(\psi)$ is the smallest congruence containing $R$, we obtain that $\ker(\psi) \subseteq \ker(\varphi)$. By the homomorphism theorem of semigroups, see e.g. [10], $A^+$ is a morphic image of $S$.

If $S$ is an F-semigroup then, by the definition of semigroup presentation, the congruence generated by $R \subseteq X^+ \times X^+$ is a nuclear congruence and it is clearly the smallest such congruence. This yields the second statement. □

The converse of the above result does not hold. Indeed, there are rather simple F-semigroups, e.g. the semigroup $\{a, aba, baba, baab\}^+$ from Markov [15], that have no finite presentations. However, by Lemma 2.1, all finitely generated F-semigroups do have finite F-presentations. By Lemma 2.1, we have also an effective solution of the *synthesis problem* which asks to find an F-presentation for a given finitely generated F-semigroup.

**Theorem 3.3.** *Each finitely generated F-semigroup $A^+ \subseteq \Sigma^+$ has a finite F-presentation that can be effectively found.*

**Example 3.4.** Let $S_1 = \{ab, a, ba\}^+$ and $S_2 = \{aaab, aa, abaa\}^+$ be two F-semigroups in $\{a, b\}^+$. They have a common F-presentation $[x, y, z; xy = yz]$. Here $X = \{x, y, z\}$, and the corresponding bijections are given by the natural orders of the semigroups $S_1$ and $S_2$.

There is a crucial difference between the semigroup presentations and the F-presentations of F-semigroups. Indeed, given any alphabet $X$ and a relation $R \subseteq X^+ \times X^+$, there exists a semigroup with the presentation $\langle X; R \rangle$, but such a pair need not define an F-presentation. This is due to the fact that the nuclear congruences of $X^+$ are not closed under intersection. We illustrate this situation in the following example.

**Example 3.5.** (1) Consider $X = \{x, y\}$ and $R = \{(xy, yx)\}$. It is clear that $\langle X; R \rangle$ is a presentation of a 2-generator free commutative semigroup. However, $[X; R]$ is not an F-presentation of any F-semigroup. To see this, assume to the contrary that $A^+ = [X; R]^\varphi$ for some F-semigroup $A^+ \subseteq \Sigma^+$. Since now $\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$, it follows that there exists a primitive word $w \in \Sigma^+$ such that $\varphi(x) = w^k$ and $\varphi(y) = w^t$ for some $k, t \geq 1$. However, now $(x^t, y^k)$ is a relation of $A^+$ in its F-presentation, that is, $\varphi(x^t) = \varphi(y^k)$. But $\ker(\varphi)$ and $\{(xy, yx)\}$ are not equivalent.

(2) An even more striking example is the presentation $\langle X; R \rangle$ with $X = \{x\}$ and $R = \{(x^3, x)\}$. The semigroup with this presentation has just one generator $a$ and it has two elements, $a$ and $a^2$. It is clear that no F-semigroup has the F-presentation $[X; R]$.

## 4. Decidable problems

Example 3.5 proposes a natural problem, namely the *analysis problem*: given a relation $R \subseteq X^+ \times X^+$, determine an F-semigroup presented by $[X; R]$, if it exists. For this problem we have only a partial solution even in the case, where $R$ is finite.

**Theorem 4.1.** *Given finite $X$ and $R \subseteq X^+ \times X^+$, finding an F-semigroup F-presented by $[X;R]$ is recursively enumerable.*

To prove Theorem 4.1, we use an exhaustive search on the finite sets of words as generating sets of F-semigroups, and, then the next theorem implies the claim, since we can always check whether a given finitely generated F-semigroup $A^+$ has the presentation $[X;R]$.

**Theorem 4.2.** *It is decidable whether or not a finitely generated F-semigroup $A^+$ has a given presentation $[X;R]$ for finite $X$ and $R \subseteq X^+ \times X^+$.*

**Proof.** Assume $\varphi : X \to X$ is a bijection. Since both $A$ and $X$ are finite sets, there are only finitely many such bijections. The congruence $\ker(\varphi)$ is a rational relation by Lemma 2.1, and thus it is sufficient to show that the problem whether a rational relation $K$ is equivalent to $R$ is decidable. This problem reduces, again by Lemma 2.1, to checking whether two finite relations $K_0$ and $R$ are equivalent. The latter problem was shown to be decidable in [5] by using Makanin's result, which states that one can effectively test whether an equation has a solution in a free semigroup. □

The analysis problem for finite F-presententation is still open:

**Problem 1.** *For given finite $X$ and $R \subseteq X^+ \times X^+$ is it decidable whether or not $[X;R]$ is an F-presentation of an F-semigroup?*

We shall now turn to one of the basic algebraic decision problems, namely the isomorphism problem of F-semigroups. This problem asks whether two F-semigroups satisfy exactly the same relations in their F-presentations, and therefore due to Lemma 2.1, and the known fact that the equivalence problem for rational relations is undecidable (see [2]), the following result sounds surprising.

**Theorem 4.3.** *The isomorphism problem for finitely generated F-semigroups is decidable.*

**Proof.** Let $A^+$ and $B^+$ be two F-semigroups. Here we may clearly suppose that $A$ and $B$ are the minimal generating sets for $A^+$ and $B^+$, respectively. If $A$ and $B$ have different cardinalities, then obviously $A^+$ and $B^+$ are not isomorphic. Assume then that $X$ is an alphabet having the same cardinality as $A$ and $B$. By Lemma 2.2, $A^+$ and $B^+$ are isomorphic if and only if they have a common F-presentation. This, in turn, holds if and only if there exist bijections $\varphi : X \to A$ and $\psi : X \to B$ such that $\ker(\varphi) = \ker(\psi)$. This latter condition is decidable, since we may construct finite equivalent subrelations $K_0 \subseteq \ker(\varphi)$ and $P_0 \subseteq \ker(\psi)$ by Lemma 2.1, and then we have to check only that $K_0 \subseteq \ker(\psi)$ (i.e., $\psi(u) = \psi(v)$ for all $(u,v) \in K_0$) and $P_0 \subseteq \ker(\varphi)$ (i.e., $\varphi(u) = \varphi(v)$ for all $(u,v) \in P_0$). □

It is an open problem whether the previous result can be extended to F-semigroups generated by rational sets.

**Problem 2.** *Is it decidable whether or not two F-semigroups $A^+$ and $B^+$ generated by rational sets A and B are isomorphic?*

Note that it is undecidable for two given rational relations $\tau_1$ and $\tau_2$ whether for all words $u$ from their domain there exists a word $v$ such that $(u,v) \in \tau_1$ and $(u,v) \in \tau_2$, see [11]. On the other hand, the freeness problem of F-semigroups is a special case of the isomorphism problem, and, as is well known, the freeness problem is not essentially more difficult to decide for rational generating sets than for finite ones; see [3].

An F-semigroup $A^+$ is *embeddable* into an F-semigroup $B^+$, if $A^+$ is isomorphic to a subsemigroup of $B^+$. If an F-semigroup $B^+$ is not periodic, that is, it does not consist of some powers of a word, then it contains a free semigroup generated by two elements, and, in this case, all F-semigroups $A^+ \subseteq \Sigma^+$ with finite $\Sigma$ are embeddable into $B^+$. This gives us

**Theorem 4.4.** *It is decidable for given finitely generated F-semigroups $A^+$ and $B^+$ whether $A^+$ is embeddable in $B^+$.*

## 5. Undecidability results

In this section we prove two natural undecidable properties of F-semigroups. The first of these relates presentations and F-semigroups.

**Theorem 5.1.** *It is undecidable whether or not a finitely presented semigroup is an F-semigroup.*

**Proof.** This is a direct corollary to a result of Markov [14], which states that it is undecidable whether a finitely presented semigroup satisfies a property $P$ such that

(1) $P$ is closed under isomorphisms, and taking subsemigroups;

(2) there exists a finitely presented $S$ that does not possess $P$;

(3) there exists a finitely presented $S$ that possesses $P$.

Clearly, the property of being an F-semigroup satisfies the Markov conditions, and thus the claim follows. □

In contrast to the isomorphism problem of finitely generated F-semigroups, we have the following undecidability result. Here, for given $A^+ = [X; R_1]^\varphi$ and $B^+ = [X; R_2]^\psi$, we ask whether there exists a relation $(u,v)$ of $A^+$ and $B^+$, with $u \neq v$, such that $\varphi(u) = \varphi(v)$ and $\psi(u) = \psi(v)$, that is, whether there exists a nontrivial relation in the F-presentations of these F-semigroups.

**Theorem 5.2.** *It is undecidable whether or not two given finitely generated F-semigroups have a common nontrivial relation in their F-presentations.*

**Proof.** In order to prove the claim we show that it is undecidable whether for two morphisms $\varphi, \psi : X^+ \to \Sigma^+$ there exist different words $u$ and $v$ such that $(u,v) \in \ker(\varphi)$ and $(u,v) \in \ker(\psi)$. The claim follows then from this when we consider the F-semigroups generated by $A = \{\varphi(a) \mid a \in X\}$ and $B = \{\psi(a) \mid a \in X\}$, since here the mappings $\varphi : X \to A$ and $\psi : X \to B$ can be assumed to be bijections.

We reduce the Post Correspondence Problem for injective morphisms to this problem. It is known that this variant of PCP is undecidable; see [13], so that our result follows.

For this, let $\gamma : \Delta^+ \to \Gamma^+$ be an injective morphism, where without restriction we may assume that $\Delta \cap \Gamma = \emptyset$. Further, let

$$\Sigma = \Gamma \cup \{c, d, e\} \quad \text{and} \quad Y = \Delta \cup \Sigma.$$

Define a morphism $\ell$ by $\ell(a) = da$ for all $a \in \Delta$. For each $a \in \Delta$, let

$$X = Y \cup \{\bar{a}\},$$

and define a new morphism $\gamma_a : X^+ \to \Sigma^+$ as follows:

$$\gamma_a(x) = \begin{cases} c \cdot \ell\gamma(a) & \text{if } x = \bar{a}, \\ \ell\gamma(x) & \text{if } x \in \Delta, \\ xd & \text{if } x = c \text{ or } x \in \Gamma, \\ de & \text{if } x = d, \\ e & \text{if } x = e. \end{cases}$$

One obtains immediately that for all $w \in \Gamma^+$,

$$d\gamma_a(w) = \ell(w)d. \tag{3}$$

Let $(u,v)$ be a *minimal pair*, that is, assume that $u$ and $v$ are two different words of minimal lengths such that $\gamma_a(u) = \gamma_a(v)$. In particular, the first letters $\mathrm{pref}_1(u)$ and $\mathrm{pref}_1(v)$ of $u$ and $v$, respectively, are different. By symmetry, we may suppose that $\mathrm{pref}_1(u) \neq c$. First we prove that

$$u \in \bar{a}\Delta^+ d \quad \text{and} \quad v \in c\Gamma^+ e. \tag{4}$$

By assumption, $\mathrm{pref}_1(u) \neq \mathrm{pref}_1(v)$, and clearly, either $\mathrm{pref}_1(u) = \bar{a}$ and $\mathrm{pref}_1(v) = c$, or both $\mathrm{pref}_1(u), \mathrm{pref}_1(v) \in \Delta$. The latter case is easily shown to yield a contadiction, since if $w_1, w_2 \in \Delta^+$ are any two words such that $\gamma_a(w_1)$ is a prefix of $\gamma_a(w_2)$, then $(\gamma_a(w_1))^{-1}\gamma_a(w_2) \in d\Gamma^+$, and this would imply that $u, v \in \Delta^+$ contradicting the injectivity of $\gamma$.

Suppose thus that $\mathrm{pref}_1(u) = \bar{a}$ and $\mathrm{pref}_1(v) = c$. We obtain now that $(\gamma_a(c))^{-1}\gamma_a(\bar{a}) \in (\Gamma d)^+\Gamma$, and hence $v$ begins with a word $v_1$, where $v_1 \in c\Gamma^+$, and $(\gamma_a(\bar{a}))^{-1}\gamma_a(v_1) = d$. Assume that we have already shown that $u$ has a prefix $u_i \in \bar{a}\Delta^+$ and $v$ has a prefix $v_i \in c\Gamma^+$ such that $(\gamma_a(u_i))^{-1}\gamma_a(v_i) = d$. Now, $u$ begins either with $u_{i+1} = u_i b$ for

some $b \in \Delta$, or with $u_i d$. In the latter case we are done: $u = u_i d$ and $v = v_i e$. In the former case, $(\gamma_a(v_i))^{-1}\gamma_a(u_{i+1}) \in (\Gamma d)^+\Gamma$, and thus $v$ begins with $v_{i+1} = v_i v'$, where $v' \in \Gamma^+$ is such that $(\gamma_a(u_{i+1}))^{-1}\gamma_a(v_{i+1}) = d$. Thus, an induction argument shows that (4) holds.

By (4), $u = \bar{a}wd$ and $v = cw'e$ for some $w \in \Delta^+$ and $w' \in \Gamma^+$. Hence,

$$\gamma_a(u) = c \cdot \ell\gamma(a) \cdot \ell\gamma(w) \cdot de = c \cdot \ell\gamma(aw) \cdot de,$$

and, using (3),

$$\gamma_a(v) = cd \cdot \gamma_a(w') \cdot e = c \cdot \ell(w') \cdot de.$$

Since $\gamma_a(u) = \gamma_a(v)$, we obtain that $w' = \gamma(aw)$, and, consequently,

$$u = \bar{a}wd, \quad v = c \cdot \gamma(aw) \cdot e \quad \text{and} \quad \gamma_a(u) = c \cdot \ell\gamma(aw) \cdot de = \gamma_a(v). \tag{5}$$

We apply now the above argumentation to two injective morphisms $\alpha, \beta : \Delta^+ \to \Gamma^+$.

Suppose first that $aw$ is a minimal solution to the PCP with the instance $(\alpha, \beta)$ for some letter $a \in \Delta$ and word $w \in \Delta^+$. Let $\varphi = \alpha_a$ and $\psi = \beta_a$ be defined as $\gamma_a$ above. Denote $u = \bar{a}wd$ and $v = c \cdot \alpha(aw) \cdot e$ $(= c \cdot \beta(aw) \cdot e)$. Now,

$$\varphi(u) = \alpha_a(\bar{a}wd) = c \cdot \ell\alpha(aw) \cdot de,$$

and, using (3),

$$\varphi(v) = \alpha_a(c\alpha(aw)e) = cd \cdot \alpha_a(\alpha(aw)) \cdot e = c \cdot \ell\alpha(aw) \cdot de,$$

and therefore $\varphi(u) = \varphi(v)$. Similarly,

$$\psi(u) = c \cdot \ell\beta(aw) \cdot de = \psi(v),$$

Therefore there exist $u$ and $v$ as required.

On the other hand, assume $\varphi(u) = \varphi(v)$ and $\psi(u) = \psi(v)$ for some $u \neq v$. We first conclude that there exists such a pair $(u, v)$ that is minimal for both $\varphi$ and $\psi$. Indeed, if $(u, v)$ is not minimal with respect to, say $\varphi$, then $u = u_1u_2$ and $v = v_1v_2$, where $(u_1, v_1)$ is a minimal pair, and in particular, $\varphi(u_1) = \varphi(v_1)$ and thus also $\varphi(u_2) = \varphi(v_2)$. By (4), $u_1 \in \bar{a}\Delta^+d$ and $v_1 \in c\Gamma^+e$, and this implies immediately that also $\psi(u_1) = \psi(v_1)$. Thus, we may assume that $(u, v)$ is a minimal pair.

Further, again by symmetry, we may assume that $\mathrm{pref}_1(u) = \bar{a}$ and $\mathrm{pref}_1(v) = c$. Therefore, by (5), $\varphi(u) = c \cdot \ell\alpha(aw) \cdot de = \varphi(v)$ and $\psi(u) = c \cdot \ell\beta(aw) \cdot de = \psi(v)$ for some $w \in \Delta^+$. Now, by (4), $v \in c\Gamma^+e$, and the definitions of $\varphi$ and $\psi$ show that $\varphi(v) = \psi(v)$. Hence, also $\alpha(aw) = \beta(aw)$, proving that the instance $(\alpha, \beta)$ has a solution. □

We emphasize that the proof of Theorem 5.2 relies essentially on the undecidability of PCP for injective morphisms. However, the problem itself is not an injective variant of a more general problem.

## References

[1] M.H. Albert and J. Lawrence, A proof of Ehrenfeucht's Conjecture, *Theoret. Comput. Sci.* **41** (1985) 121–123.
[2] J. Berstel, *Transductions and Context-Free Languages* (B.G. Teubner, Stuttgart, 1979).
[3] J. Berstel and D. Perrin, *Theory of Codes* (Academic Press, New York, 1986).
[4] C. Choffrut and J. Karhumäki, Combinatorics of words, in: G. Rozenberg and A. Salomaa, eds., *Handbook of Formal Languages*, Vol. I (Springer, Berlin, 1996), to appear.
[5] K. Culik II and J. Karhumäki, Systems of equations over a free monoid and Ehrenfeucht's Conjecture, *Discrete Math.* **43** (1983) 139–153.
[6] P. Dubreil, Sur le demi-groupe des endomorhismes d'une algébre abstraite, *Lincei-Rend. Sc. Fis. mat. Nat.* 46 (1969) 149–153.
[7] V.S. Guba, The equivalence of infinite systems of equations in free groups and semigroups with finite subsystems, *Mat. Zametki* **40** (1986) 321–324 (in Russian).
[8] T. Harju and J. Karhumäki, On the defect theorem and simplifiability, *Semigroup Forum* **33** (1986) 199–217.
[9] T. Harju and J. Karhumäki, Morphisms, in: G. Rozenberg and A. Salomaa, eds., *Handbook of Formal Languages*, Vol. I (Springer, Berlin, 1996), to appear.
[10] J.M. Howie, *An Introduction to Semigroup Theory* (Academic Press, London, 1976).
[11] J. Karhumäki and Y. Maon, A simple undecidable problem: existential agreement of inverses of two morphisms on a regular language, *J. Comput. System Sci.* **32** (1986) 315–322.
[12] G. Lallement, *Semigroups and Combinatorial Applications* (Wiley, New York, 1979).
[13] M.Y. Lecerf, Récursive insolubilité de l'équation générale de diagonalisation de deux monomorphismes de monoïdes libres $\alpha x = \beta x$, *Comptes Rendus* **257** (1963) 2940–2943.
[14] A. Markov, Impossibility of algorithms for recognizing some properties of associative systems, *Dokl. Akad. Nauk SSSR* **77** (1951) 953–956 (in Russian).
[15] Al.A. Markov, On finitely generated subsemigroups of a free semigroup, *Semigroup Forum* **3** (1971) 251–258.